UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/615,676	07/14/2000	Michael P. Lyle	RECOP005	6964

21912 7590 01/21/2004

VAN PELT & YI LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	7

DATE MAILED: 01/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/615,676	LYLE ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 July 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 July 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *5,6* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-43 have been examined.

2. In the examination of the instant application, it is being presumed that the invention is being used on computerized equipment, and that "attacks" originate outside of the computer being used.

Requirement for Information

3. Applicant and the assignee of this application are required under 37 CFR 1.105 to provide the following information that the examiner has determined is reasonably necessary to the examination of this application.

The information is required to identify products and services embodying the disclosed subject matter of a simplified version of the instant invention that was submitted to MIT Lincoln Labs for an evaluation in 1998, for the article *Durst et al., "Testing and Evaluating Computer Intrusion Detection Systems," July 1999*, as referenced in Provisional U.S. Patent Application No. 60/151,531, p. 15, and, in the event that it constituted a public use, identify the properties of similar products and services found in the prior art.

Information describing to the functionality of the simplified version, including algorithms and data structures employed, and evidence of the date of its first public use are necessary in order to make a determination as to whether it should be considered prior art with respect to some or all of the claims of the instant application under 35 U.S.C. 102(b).

A user's or technical manual for the simplified version in addition to evidence establishing a date of first public use would be considered to be a sufficient response for this requirement.

The fee and certification requirements of 37 CFR 1.97 are waived for those documents submitted in reply to this requirement. This waiver extends only to those documents within the scope of this requirement under 37 CFR 1.105 that are included in the applicant's first complete communication responding to this requirement. Any supplemental replies subsequent to the first communication responding to this requirement and any information disclosures beyond the scope of this requirement under 37 CFR 1.105 are subject to the fee and certification requirements of 37 CFR 1.97.

The applicant is reminded that the reply to this requirement must be made with candor and good faith under 37 CFR 1.56. Where the applicant does not have or cannot readily obtain an item of required information, a statement that the item is unknown or cannot be readily obtained will be accepted as a complete reply to the requirement for that item.

This requirement is an attachment of the enclosed Office action. A complete reply to the enclosed Office action must include a complete reply to this requirement. The time period for reply to this requirement coincides with the time period for reply to the enclosed Office action.

Priority

4. Applicant's claim for domestic priority under 35 U.S.C. 119(e) to Provisional U.S. Patent Applications 60/143,821, filed 14 July 1999 and 60/151,531, filed 30 August 1999 is acknowledged. However, the provisional applications upon which priority is claimed fail to provide adequate support under 35 U.S.C. 112 for any of the claims of this application. Though there is a reference to a queue for processing events in 60/151,531, p.18, it is not described in a manner that is enabling with respect to how the queues would be used for intrusion detection.

Information Disclosure Statement

5. The following Information Disclosure Statement in the instant application has been fully considered:

Paper No. 6, filed 4 June 2001.

6. Paper No. 3, an IDS filed 13 November 2000, was not found in the file wrapper. Applicant is requested to furnish a replacement copy, if available, along with a copy of the return receipt postcard.

7. The two items in Paper No. 5, the IDS filed 13 November 2000, were not found. New copies have been printed and added to the file, and have been fully considered.

Drawings

8. The drawings are objected to as failing to comply with 37 CFR 1.84(g) because the margins are outside the specified limits. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

9. The drawings are objected to as failing to comply with 37 CFR 1.84(l) because the lines are not uniformly thick and well-defined, and because numerous labels are illegible. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

10. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(1) because numerous reference characters are illegible. A proposed drawing correction or

corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

11. Applicant is reminded of the proper content of an abstract of the disclosure.

A patent abstract is a concise statement of the technical disclosure of the patent and should include that which is new in the art to which the invention pertains. If the patent is of a basic nature, the entire technical disclosure may be new in the art, and the abstract should be directed to the entire disclosure. If the patent is in the nature of an improvement in an old apparatus, process, product, or composition, the abstract should include the technical disclosure of the improvement. In certain patents, particularly those for compounds and compositions, wherein the process for making and/or the use thereof are not obvious, the abstract should set forth a process for making and/or use thereof. If the new technical disclosure involves modifications or alternatives, the abstract should mention by way of example the preferred modification or alternative.

The abstract should not refer to purported merits or speculative applications of the invention and should not compare the invention with the prior art.

Where applicable, the abstract should include the following:
(1) if a machine or apparatus, its organization and operation;
(2) if an article, its method of making;
(3) if a chemical compound, its identity and use;
(4) if a mixture, its ingredients;
(5) if a process, the steps.

Extensive mechanical and design details of apparatus should not be given.

The abstract does not adequately encompass the breadth of the disclosure or claims.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. Claim 18 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "known to be vulnerable to attack" is a relative term which renders the claim indefinite. The term "known to be vulnerable to attack " is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 1-4, 7-11, 20, 21, 23, 24, 31-34, and 41-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,881 to Conklin et al. in view of Knuth, "The Art of Computer Programming, Volume 1," 2nd Edition, 1973, pp. 234-238.

Regarding claims 1, 42, and 43, the network surveillance system disclosed by Conklin monitors intrusion detections.

Conklin does not disclose the method by which incoming events are stored while awaiting processing.

Knuth discloses that queues are used to allow the processing of exception conditions in a set of data (see p.236, last paragraph and p.237, first paragraph).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the system of Conklin by using queues, as disclosed by Knuth, in order to allow the processing of exception conditions in a set of data.

As per claims 2-4 and 7-11, the system disclosed by Conklin may respond by automatically sending an alert message to a network management system (which is trusted) using Trap PDUs (see column 5, lines 46-60).

As per claims 20, 21, 23, and 24, the system classifies data by the type of event, processing successive sets of data (see column 6, lines 1-12).

As per claim 31, attack checks are comparative, and different events are therefore associated with one another (see column 7, lines 51-55).

As per claim 32, pattern matching is used, therefore allowing events with the same message to be correlated.

As per claim 33, incoming packets are also correlated with historical data.

As per claim 34, source IP addresses are reported (see column 5, lines 29-30).

As per claim 41, collected data is stored in a database (see column 4, line 61 to column 5, line 9).

14. Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,881 to Conklin et al. in view of Knuth, "The Art of Computer Programming, Volume 1," 2nd Edition, 1973, pp. 234-238 as applied to claim 4 above, and further in view of U.S. Patent No. 6,311,274 to Day.

Conklin and Knuth only disclose event notifications via SNMP traps.

The network alert system disclosed by Day includes alert notifications in the event of network intrusions via email or pager (see column 5, lines 33-55), and suggests the necessity of performing an appropriate alert action in response to the alert message.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Conklin and Knuth by implementing an alert system that might send notifications by pager or email, due to the necessity of performing an appropriate alert action in response to the alert message.

15. Claims 12-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,881 to Conklin et al. in view of Knuth, "The Art of Computer Programming, Volume 1," 2nd Edition, 1973, pp. 234-238 as applied to claim 1 above, and further in view of U.S. Patent No. 6,067,620 to Holden et al.

Regarding claims 12-14, Conklin and Knuth do not disclose the direct monitoring or manipulation of network ingress and egress ports.

The security device disclosed by Holden includes a hardware SNIU, a network interface that is placed on every network interface in a system that is connected to an untrusted network (such as computers, routers, switches, etc.) and diverts incoming data to a set of secure modules to process packets (constituting a copy port). A network of SNIU-equipped machines creates a global security perimeter.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Conklin and Knuth by using the SNIU disclosed by Holden on all network interfaces, in order to create a global security perimeter.

As per claim 15, Conklin discloses internal network communications using SNMP, a network management protocol.

As per claims 16-19, Conklin discloses the scanning of packets for contents (such as strings) and monitors services that are vulnerable, such as telnet (see column 2, line 64 to column 3, line 14).

16. Claims 22, 25-27, 30, 39, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,881 to Conklin et al. in view of Knuth, "The Art of Computer Programming, Volume 1," 2nd Edition, 1973, pp. 234-238 as applied to claims 1 and 24 above, and further in view of U.S. Patent No. 5,574,912 to Hu et al.

Conklin and Knuth do not disclose the use of more than one queue.

The lattice scheduler disclosed by Hu includes places processes within a lattice of queues for processing, with the indices depending upon attributes of the processes being placed, that are then executed in a round-robin manner, with subsequent queues being used when queues are exhausted (see column 8, line 50 to column 9, line 8). Hu further suggests that this is done to achieve better CPU utilization (see column 5, lines 32-35).

17. Claims 28 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,881 to Conklin et al. in view of Knuth, "The Art of Computer Programming, Volume 1," 2nd Edition, 1973, pp. 234-238 further in view of U.S. Patent No. 5,574,912 to Hu et al. as applied to claim 27 above, and further in view of U.S. Patent No. 6,233,686 to Zenchelsky et al.

Conklin, Knuth, and Hu do not disclose the hashing of string data or IP addresses in order to derive the table indices in which data is to be inserted.

The network access control system of Zenchelsky includes the hashing of network addresses (see abstract), which are IP addresses, or string data (see column 6, line 60 to column 7, line 5) for determining table indices, and suggests that hash tables are used to allow more efficient searching.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Conklin, Knuth, and Hu by organize the matrix of queues as hash tables, using network addresses and/or string contents, as hash tables are used to allow more efficient searching.

18. Claims 36-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,991,881 to Conklin et al. in view of Knuth, "The Art of Computer Programming, Volume 1," 2nd Edition, 1973, pp. 234-238 as applied to claim 35 above, and further in view of U.S. Patent No. 6,442,694 to Bergman et al.

Conklin and Knuth do not disclose the tracing back to determine the point of attack.

The fault isolation system disclosed by Bergman uses a network map mapping all the nodes in a network, stored at each system, wherein, upon detection of an attack at a node, the attack is iteratively traced back to the point at which it entered the network see column 14, line 59 to column 19, line 20). Bergman further suggests that it would be desirable to provide a technique for localizing an attack on a network (see column 7, lines 55-62).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Conklin and Knuth by using the fault isolation technique disclosed by Bergman to trace back attacks, in order to localize an attack on a network.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11

F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

19. Claims 1, 20, and 41-43 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 6,647,400 to Moran in view of Knuth, "The Art of Computer Programming, Volume 1," 2nd Edition, 1973, pp. 234-238.

Although the conflicting claims are not identical, they are not patentably distinct from each other because the system claimed by Moran received data for the purpose of detection an intrusion (attack) and classifies the data.

Moran does not claim the use of queues.

Knuth discloses that queues are used to allow the processing of exception conditions in a set of data (see p.236, last paragraph and p.237, first paragraph).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the system of Moran by using queues, as disclosed by Knuth, in order to allow the processing of exception conditions in a set of data.

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 5,485,409 to Gupta et al. discloses a system for analyzing network vulnerabilities.

U.S. Patent No. 6,141,686 to Jackowski et al. discloses a network traffic classifier for policy enforcement.

U.S. Patent No. 6,408,391 to Huff et al. discloses a Pattonesque approach to detecting and reacting to system penetrations.

U.S. Patent No. 6,499,107 to Gleichauf et al. discloses a method for correlating sets of incoming packets.

U.S. Patent No. 6,578,147 to Shanklin et al. discloses a system for detecting intrusions that uses load balancing.

U.S. Statutory Invention Registration H1944 to Cheswick et al. discloses a client-based firewall.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (703) 305-7727. The examiner can normally be reached on Monday-Thursday from 8:00 AM - 4:00 PM Eastern Time. The examiner can also be reached on alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703) 872-9306
Hand-delivered responses should be brought to Crystal Park 2, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

MEH

January 12, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100